



IPv6 mit Unix

Ein Crashkurs

Benedikt Stockebrand

`me@benedikt-stockebrand.de`

GUUG Sage Rhein/Main, Darmstadt, 10.11.2005



Themen

- Warum IPv6?
- Grundlagen
- Automatische Adresskonfiguration
- IPv6 im DNS
- Routing
- Essentielle Anwendungsprotokolle



Warum IPv6?

- Probleme mit IPv4 und ihre Lösung mit IPv6
 - Adressknappheit
 - End-to-End-Connectivity contra NAT
 - Aufwendige Adresskonfiguration
 - Aufwendige Änderungen der Adressprefixe
 - Eingeschränkte Multicast-Unterstützung
 - Broadcasts
 - Übergroße Routing-Tabellen
- Neue Features
 - Verschlüsselung mit IPsec ist Kernbestandteil
 - Mobile IPv6
 - Quality of Service (QoS)

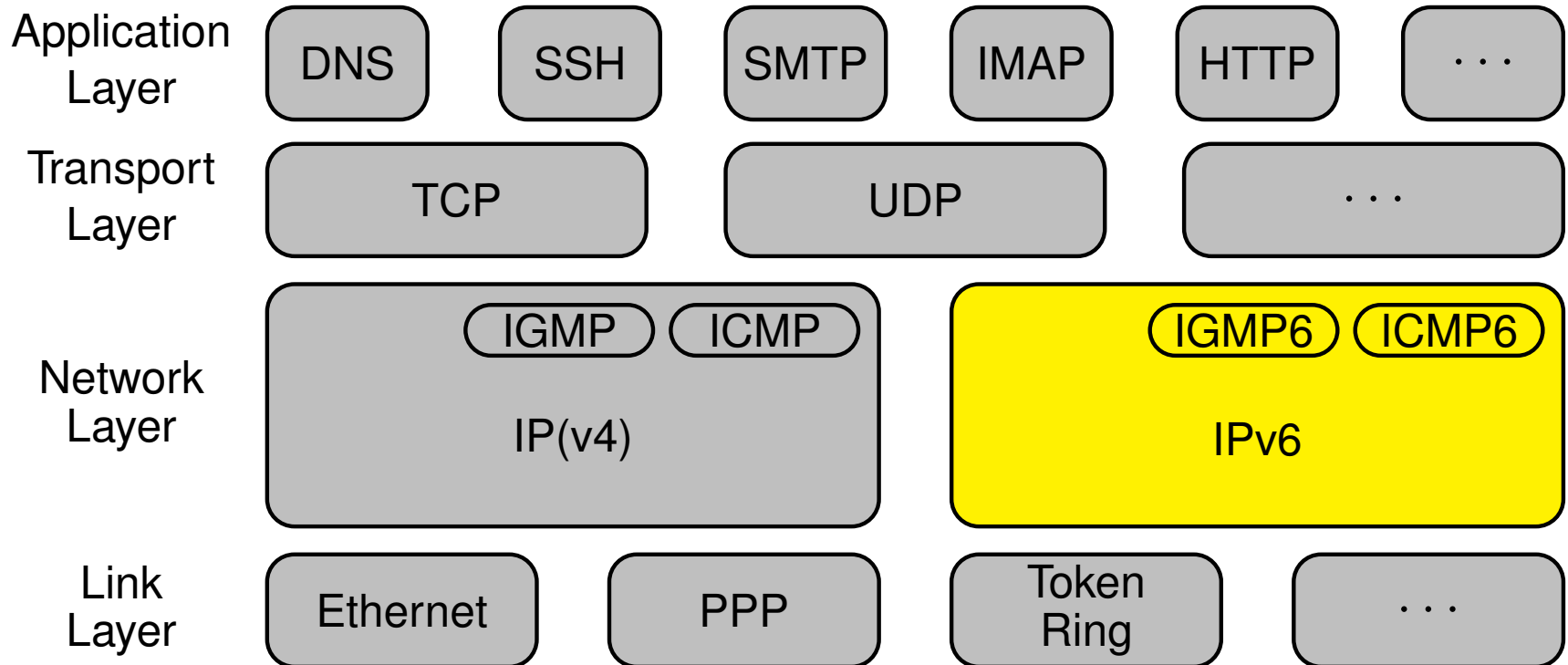


Grundlagen

Grundlagen

- Einordnung im TCP/IP-Stack
- Aufbau von IPv6-Adressen
- Adress-Scopes und warum sie nicht den RFC1918-Adressen entsprechen
- Erweitertes/verbessertes Multicast
- Anycast

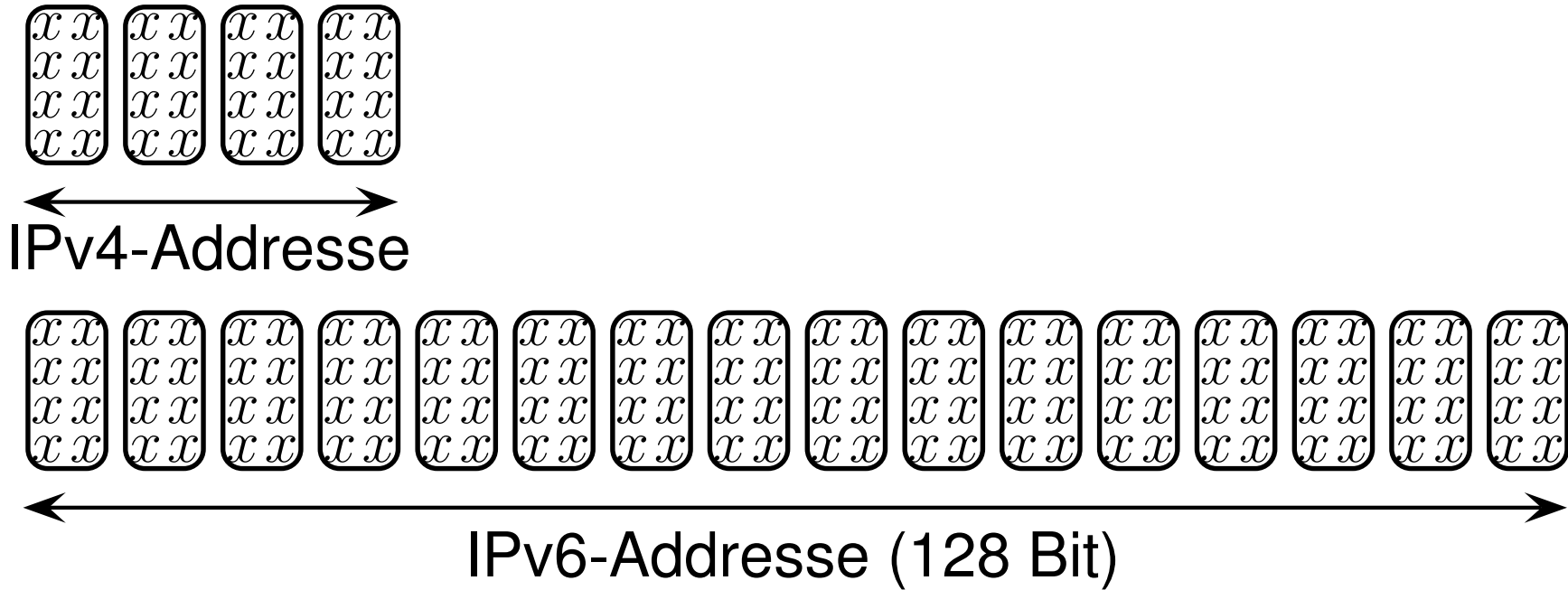
Grundlagen – IPv6 im TCP/IP-Stack



Grundlagen – IPv6 im TCP/IP-Stack II

- TCP, UDP etc. bleiben unverändert
 - Software-Portierung ist im allgemeinen einfach
 - Es gibt kein echtes „TCPv6“ (aber „TCP/IPv6“)
- IPv6 läuft parallel zu IPv4
 - Legacy-Systeme erfordern „nur“ zusätzlichen Administrationsaufwand
 - Es gibt kein „großes Umschalten“
 - Eine sanfte Migration ist möglich – und sinnvoll!

Grundlagen – IPv6-Adressen



Grundlagen – IPv6-Adressen II

Anzahl Adressen:

$$2^{128} = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,456$$

$$\approx 3.4 \times 10^{38}$$

Grundlagen – IPv6-Adressen II

Anzahl Adressen:

$$2^{128} = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,456$$

$$\approx 3.4 \times 10^{38}$$

Verhältnis von IPv6- zu IPv4-Adressen:

$$2^{96} = 79\,228\,162\,514\,264\,337\,593\,543\,950\,336 \approx 8 \times 10^{29}$$

Grundlagen – IPv6-Adressen II

Anzahl Adressen:

$$2^{128} = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,456$$

$$\approx 3.4 \times 10^{38}$$

Verhältnis von IPv6- zu IPv4-Adressen:

$$2^{96} = 79\,228\,162\,514\,264\,337\,593\,543\,950\,336 \approx 8 \times 10^{29}$$

Verhältnis von IPv6-Site-Prefixen (/48) zu IPv4-/24-Prefixen:

$$2^{24} = 16\,777\,216 \approx 1.7 \times 10^7$$

Grundlagen – IPv6-Adressen II

Anzahl Adressen:

$$2^{128} = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,456$$
$$\approx 3.4 \times 10^{38}$$

Verhältnis von IPv6- zu IPv4-Adressen:

$$2^{96} = 79\,228\,162\,514\,264\,337\,593\,543\,950\,336 \approx 8 \times 10^{29}$$

Verhältnis von IPv6-Site-Prefixen (/48) zu IPv4-/24-Prefixen:

$$2^{24} = 16\,777\,216 \approx 1.7 \times 10^7$$

Es gibt genug Adressen für alles und jeden!

Grundlagen – Adressnotation

- In Hexadezimal
- In Blöcken aus zwei Bytes/Octets, also vier Ziffern
- Blöcke mit Doppelpunkt getrennt

```
fe80:0000:0000:0000:020c:f1ff:fed:d2be
```

- Ohne führende Nullen in den Blöcken

```
fe80:0:0:0:20c:f1ff:fed:d2be
```

- Mit *einem* Doppel-Doppelpunkt für mehrere Null-Blöcke

```
fe80::20c:f1ff:fed:d2be
```

Grundlagen – Adressnotation II

- Prefixe wie bei IPv4 mit Adresse, Slash und der Anzahl Bits in dezimal:

`fe80::/64`

- Gemischte Notation aus 96 Bit IPv6-Prefix und IPv4-Adresse:

`::ffff:127.0.0.1`

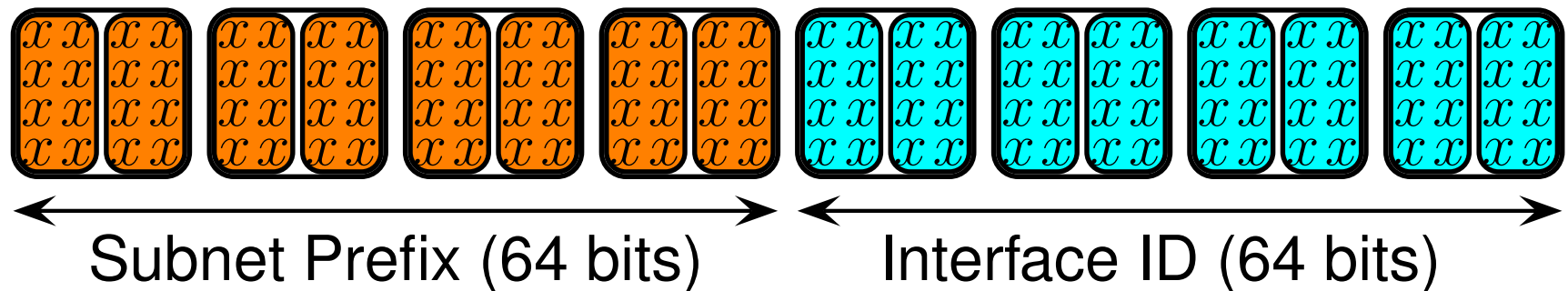
- Base-85-Encoding gemäß RFC 1924 (1. April 1996)

Grundlagen – Scopes

- Einführung von Scopes zur Begrenzung der Reichweite
- Globaler Scope
- Site-Local Scope
- Link-Local Scope
- Interface-Local Scope
- **Site-Local-Adressen sind NICHT für eine Neuauflage von NAT gedacht!**

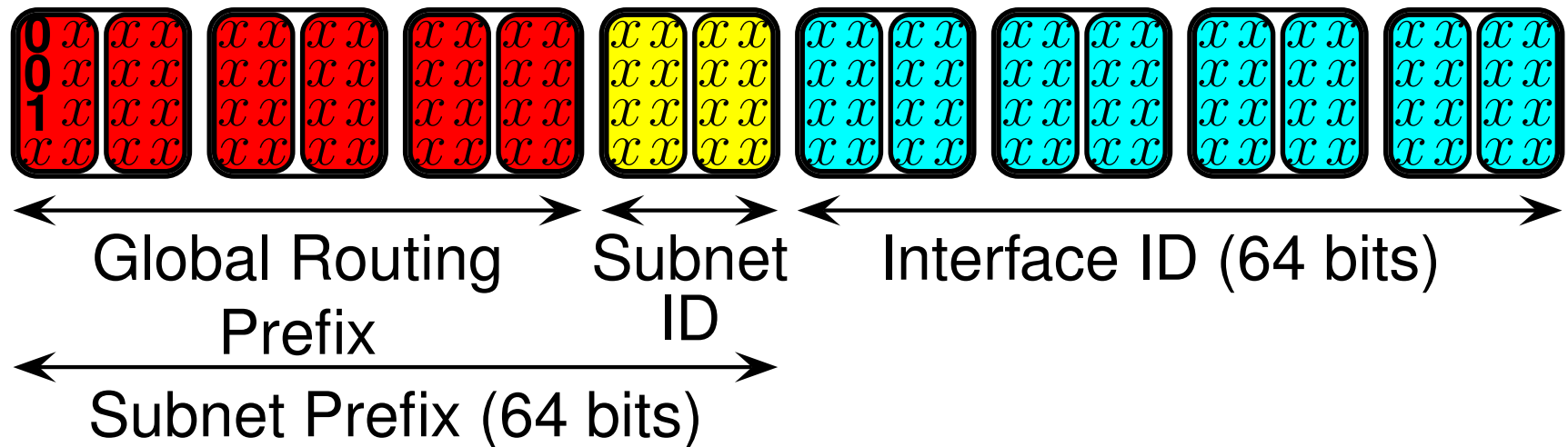
Grundlagen – Unicast-Adressen

- Besondere Adressen:
 - Die “Unspecified Address” ($::$)
 - Die Loopback-Adresse ($::1$)
- Normale Adressen:



Grundlagen – Unicast-Adressen II

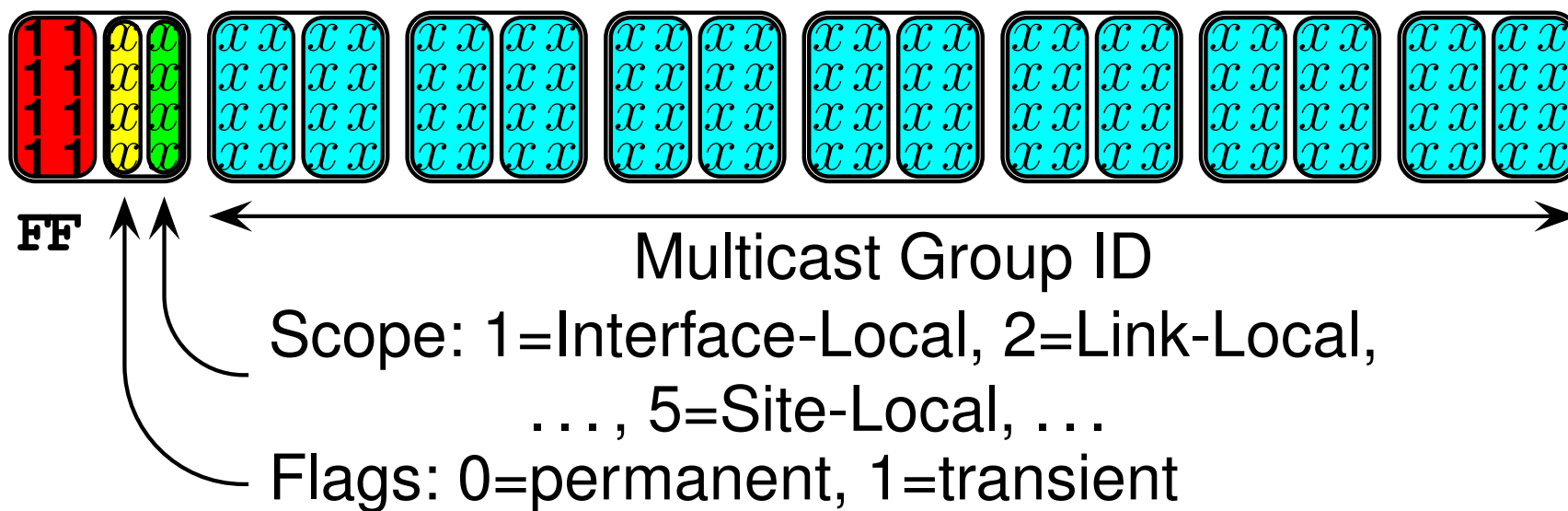
- Global geroutete Unicast-Adressen ($2000::/3$)



- Site-Local-Adressen ($\text{fec}0::/10$) — „Deprecated“
- Unique-Local-Adressen
 - Zentral verwaltet ($\text{fc}00::/8$)
 - Zufällig ausgewählt ($\text{fd}00::/8$)
- Link-Local-Adressen ($\text{fe}80::/10$)

Grundlagen – Multicast-Adressen

- Von Anfang an vorgesehen
- Per Protocol-Independent Multicast (PIM) geroutet
- Noch weitere Scopes zur freien Verfügung
- Ersetzt Broadcasts



Grundlagen – Multicast-Adressen II

- `ff02::1` – All-Nodes Link-Local Multicast Address
- `ff02::2` – All-Routers Link-Local Multicast Address
- `ff02::1:ffxx:xxxx` – Solicited Node Multicast Address



Grundlagen – Anycast


- Benutzt Unicast-Adressen
- Mehrere Listener hören auf die Adresse
- Ein Paket geht nur an *einen* der Listener
- Bisher noch experimentell, nicht allgemein nutzbar
- Fest zugewiesen: Subnet-Router Anycast Address, Interface ID 0:0:0:0

Interne Änderungen gegenüber IPv4

Interne Änderungen gegenüber IPv4

- Neighbor Discovery als Layer-2-unabhängiger ARP-Nachfolger
- Duplicate Address Detection
- Verbesserte Timeout-Mechanismen
- Kleine IP-Header durch viele mögliche Option Headers
- Optimierte Prüfsummen
- Prüfsummenkontrolle nur an den Endpunkten
- Path MTU Discovery zwingend vorhanden
- Fragmentierung nur beim Absender
- Für Router-Durchsatz optimiert
- ...

Aufbau des IPv6-Base-Headers (RFC 2460)



Vers.	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			



Dipl.-Inform. Benedikt Stockebrand

<http://www.benedikt-stockebrand.de/>

Automatische Adresskonfiguration

Automatische Adresskonfiguration

- Statische Adresskonfiguration weiter möglich
- Stateless Address Autoconfiguration (SAC) bevorzugt
- “DHCP without the Pains”
- Address Renumbering im laufenden Betrieb

SAC – Nodes, Routers, Hosts

Node Alles, was IPv6 spricht

Router Ein Node, der Pakete für andere annimmt und weiterleitet

Host Ein Node, aber kein Router

SAC – Ein Host-Interface fährt hoch

So fährt ein Host-Interface hoch:

1. Interface wählt eine Interface ID
2. Interface konfiguriert damit Link-Local-Adresse
3. Interface macht Duplicate Address Detection (DAD)
4. Interface fragt per Multicast alle Router nach Prefixen
5. Interface konfiguriert *alle* Prefixe zusammen mit seiner Interface ID als Adresse
6. Interface konfiguriert *alle* Router als Defaultrouter

SAC – Unsolicited Router Advertisements

- Router schicken regelmäßig von sich aus Prefix- und Router-Informationen
- Ändert sich die Router-Konfiguration, aktualisieren Hosts ihre Konfiguration
- Router „verabschieden“ sich beim Shutdown vom Netz
- Ausgefallene Router werden schnell erkannt
- Prefixe ohne Router werden auskonfiguriert

SAC – Vorteile

- Prefix-Konfiguration nur auf Routern
- Redundante Router inhärent unterstützt
- Adress-Rekonfiguration im laufenden Betrieb möglich
- „Klare Verantwortlichkeiten“
 - Prefixe werden von Routern verwaltet
 - Interface IDs werden vom Node selbst verwaltet
- Kein DHCP-Server als Single Point of Failure
- Keine inkonsistenten DHCP-Lease-Datenbanken
- „Rogue DHCP“-Server bzw. „Rogue-Router“ überschreiben keine Konfigurationen in den Hosts



IPv6 im DNS

DNS – Historische Altlasten

- A6-Records statt AAAA (deprecated, unbenutzt)
- Bitstring-PTR-Records (deprecated, nur von alten dig-Versionen benutzt)
- PTR-Records ursprünglich in `ip6.int.` statt `ip6.arpa.` (deprecated, von einigen alten Resolvern benutzt)

DNS – Dynamische Updates

- Frage: Wie kommen die SAC-Adressen ins DNS?
- Antwort: Über dynamische DNS-Updates.
- Frage: Welche Implementierungen gibt es?
- Antwort: Das ist nicht Sache der Standardisierung.
- Alternative Antwort: Für Unix gibt es eine experimentelle Implementierung (auf meiner Home Page)

DNS – Implementierungen

- Aktuelle BIND 8/9-Versionen unterstützen IPv6
- Alle Resolver verstehen IPv6-Adressen
- Der WinXP-Resolver kann nicht über IPv6 den Server befragen!



Routing

Routing

- Unterscheidung zwischen Hosts und Routern nötig
- Hosts: ICMP Redirects von den Routern
- Router: Statische Routen oder dynamisches Routing

Routing – Konfiguration der Hosts

- Hosts finden Router per Stateless Autoconfiguration
- Verwalten damit Liste von Default Routern
- Bekommen von Routern ggf. ICMP Redirects
- Keine eigene Routing-Konfiguration

Routing – Statisches Routing

- Routen können wie bei IPv4 statisch gesetzt werden
- Keine grundlegenden Änderungen gegenüber IPv4

Routing – Dynamisches Routing

- RIPng: IPv6-Variante von RIPv2
 - Für gängige Unixe verfügbar
 - Nicht mit WinXP
- OSPFv3: OSPFv2 für IPv6
 - Setzt entsprechende Software voraus
 - Eher mit Router-Hardware üblich
- EIGRP (unüblich/in Entwicklung)
- BGP
 - Benutzt die Multiprotokoll-Erweiterungen
- IS-IS (unüblich/in Entwicklung)

Routing – Statisch oder dynamisch?

- Generell gleiche Überlegungen wie bei IPv4
- Aber tendenziell eher dynamisches Routing
 - Hosts sind nicht betroffen
 - Hosts können nicht „stören“
 - Absicherung durch IPsec prinzipiell möglich
 - Bessere Redundanz möglich



Essentielle Anwendungsprotokolle

Secure Shell (Ssh)

- Funktioniert problemlos mit IPv6
- Keine Änderungen in der Konfiguration nötig
- Ggf. mit `ListenAddress` in `sshd_config` steuerbar



HTTP über IPv6

- IPv6-Support im Apache erst ab Version 2
- Kein stabiler IPv6-Support in Squid
- Proxy-Modul in Apache, FFProxy als Alternative zu Squid

E-Mail (SMTP)

- Exim: Etwas ungewöhnliche Syntax in der Konfiguration
- Sendmail: Muss ggf. passend konfiguriert werden
- Postfix: Funktioniert problemlos



Weiterführende Themen



IPv4/IPv6-Interaktion

- Application Gateways/Proxies: Verbinden IPv4 und IPv6 auf Anwendungsebene
- Protocol Translation: Übersetzt auf IP-Ebene, ähnlich NAT



Tunnel-Mechanismen

- Verbinden IPv6-Netze über reine IPv4-Strecken
- Mehrere unterschiedliche Verfahren
- Komplexes Thema
- Muss in Paketfiltern berücksichtigt werden!

Neue Features

- Quality of Service (QoS)
 - Differentiated Services
 - Integrated Services und Resource Reservation Protocol (RSVP)
- Mobile IPv6
 - Sehr leistungsstark
 - Extrem sicherheitsrelevant!
- IPsec
 - Verbindlicher Kernbestandteil
 - Leider bei Microsoft nur mit “NULL”-Verschlüsselung



Vertiefende Lektüre

Vertiefende Lektüre

Silvia Hagen: IPv6 – Grundlagen – Funktionalität –
Integration

Sunny Edition, 2004

ISBN 3-9522942-0-9

Vertiefende Beschreibung der Protokolle

Benedikt Stockebrand: IPv6-Tutorial
iX 2–4/2005 (3 Teile)

Heise-Verlag, Hannover

Grundlagen und Einrichtung mit Unix

IETF: Requests for Comments (RFCs)

<http://www.ietf.org/>

Die offiziellen Spezifikationen